(F) ensure that all worker responses are confidential and are never shared with management; and

(G) interview a representative of the labor organization or other worker representative organization that represents workers at the facility or, if no such organization is present, attempt to interview a representative from a local worker advocacy group.

(2) MANAGEMENT INTERVIEWS.—The auditor shall—

(A) interview a cross-section of the management of the supplier, including human resources personnel, production supervisors, and others; and

(B) use audit tools to ensure that managers are asked a comprehensive set of questions.

(3) DOCUMENTATION REVIEW.—The auditor shall—

(A) conduct a documentation review to provide tangible proof of compliance and to corroborate or find discrepancies in the information gathered through the worker and management interviews; and

(B) review, at a minimum, the following types of documents:

(i) Age verification procedures and documents.

(ii) A master list of juvenile workers.

(iii) Selection and recruitment procedures.

(iv) Contracts with labor brokers, if any.

(v) Worker contracts and employment agreements.

(vi) Introduction program materials.

(vii) Personnel files.

(viii) Employee communication and training plans, including certifications provided to workers including skills training, worker preparedness, government certification programs, and systems or policy orientations.

(ix) Collective bargaining agreements, including collective bargaining representative certification, descriptions of the role of the labor organization, and minutes of the labor organization's meetings.

(x) Contracts with any security agency, and descriptions of the scope of responsibilities of the security agency.

(xi) Payroll and time records.

(xii) Production capacity reports.

(xiii) Written human resources policies and procedures.

(xiv) Occupational health and safety plans and records including legal permits, maintenance and monitoring records, injury and accident reports, investigation procedures, chemical inventories, personal protective equipment inventories, training certificates, and evacuation plans.

(xv) Disciplinary notices.

(xvi) Grievance reports.

(xvii) Performance evaluations.

(xviii) Promotion or merit increase records.

(xix) Dismissal and suspension records of workers.

(xx) Records of employees who have resigned.

(xxi) Worker pay stubs.

(4) CLOSING MEETING WITH MANAGEMENT.—The auditor shall hold a closing meeting with the management of the covered business entity to—

(A) report violations and nonconformities found in the facility; and

(B) determine the steps forward to address and remediate any problems.

(5) REPORT PREPARATION.—The auditor shall prepare a full report of the audit, which shall include—

(A) a disclosure of the direct supplier's or on-site service provider's—

(i) documented processes and procedures that relate to eradicating forced labor; and

(ii) documented risk assessment and prioritization policies as such policies relate to eradicating forced labor;

(B) a description of the worker interviews, manager interviews, and documentation review required under paragraphs (1), (2), and (3);

(C) a description of all violations or suspected violations by the direct supplier of any forced labor laws of the United States or, if applicable, the laws of another country as described in section 6132(b)(2)(B)(ii); and

(D) for each violation described in subparagraph (C), a description of any corrective and protective actions recommended for the direct supplier consisting of, at a minimum—

(i) the issues relating to the violation and any root causes of the violation;

(ii) the implementation of a solution; and

(iii) a method to check the effectiveness of the solution.

(b) ADDITIONAL REQUIREMENTS RELATING TO AUDITS.—Each covered business entity shall include, in any contract with a direct supplier or on-site service provider, a requirement that—

(1) the supplier or provider shall not retaliate against any worker for participating in an audit relating to forced labor; and

(2) worker participation in an audit shall be protected through the same grievance mechanisms available to the worker available for any other type of workplace grievance.

SEC. 6134. ENFORCEMENT.

(a) CIVIL DAMAGES.—The Secretary may assess civil damages in an amount of not more than $100,000,000 if, after notice and an opportunity for a hearing, the Secretary determines that a covered business entity has violated any requirement of section 6132(b).

(b) PUNITIVE DAMAGES.—In addition to damages under subsection (a), the Secretary may assess punitive damages in an amount of not more than $500,000,000 against a covered business entity if, after notice and an opportunity for a hearing, the Secretary determines the covered business entity willfully violated any requirement of section 6132(b).

(c) DECLARATIVE OR INJUNCTIVE RELIEF.—The Secretary may request the Attorney General institute a civil action for relief, including a permanent or temporary injunction, restraining order, or any other appropriate order, in the district court of the United States for any district in which the covered business entity conducts business, whenever the Secretary believes that a violation of section 6132(b) constitutes a hazard to workers.

SEC. 6135. REGULATIONS.

Not later than 180 days after the date of enactment of this Act, the Secretary shall promulgate rules to carry out this subtitle.

SA 1949. Mr. HAWLEY submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title V of division B, add the following:

SEC. 25___. PROHIBITION ON THE LICENSING AND TRANSFERRING OF CERTAIN INTELLECTUAL PROPERTY RIGHTS.

No intellectual property developed through research that is funded through the expenditure of Federal funds received under this division (or an amendment made by this division), or the appropriation of which are authorized under this division (or an amendment made by this division), may be licensed or transferred—

(1) to any business or research institution that is located outside of the United States; and

(2) for the commercialization or production of goods, services, or technologies.

SA 1950. Mr. HAWLEY submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. IMPOSING DATA SECURITY REQUIREMENTS AND STRENGTHENING REVIEW OF FOREIGN INVESTMENTS WITH RESPECT TO CERTAIN TECHNOLOGY COMPANIES FROM FOREIGN COUNTRIES OF CONCERN.

(a) DEFINITIONS.—In this section:

(1) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(2) COUNTRY OF CONCERN.—

(A) IN GENERAL.—Subject to subparagraph (B)(iii), the term ''country of concern'' means—

(i) the People's Republic of China;

(ii) the Russian Federation; and

(iii) any other country designated by the Secretary of State as being of concern with respect to the protection of data privacy and security.

(B) DESIGNATION OF COUNTRIES OF CONCERN.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Secretary of State shall—

(i) review the status of data privacy and security requirements (including by reviewing laws, policies, practices, and regulations related to data privacy and security) in each foreign country to determine—

(I) whether it would pose a substantial risk to the national security of the United States if the government of such country gained access to the user data of citizens and residents of the United States; and

(II) whether there is a substantial risk that the government of such country will, in a manner that fails to afford similar respect for civil liberties and privacy as the Constitution and laws of the United States, obtain user data from companies that collect user data;

(ii) designate each country that meets the criteria of clause (i) as a country of concern; and

(iii) remove the designation from any country that was previously designated a country of concern (regardless of whether such designation was pursuant to clause (i) or (ii) of subparagraph (A) or was made by the Secretary of State pursuant to clause (iii) of such subparagraph) if the country—

(I) no longer meets the criteria of clause (i); and

(II) is not at substantial risk of meeting such criteria.

(C) REGULATIONS.—Not later than 90 days after the date of the enactment of this Act, the Secretary of State shall prescribe regulations—